UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,829	07/10/2003	Franck Le	1135.41904X00	8920

20457 7590 05/18/2007

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-3873

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
05/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/615,829	LE ET AL.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 02/12/07. The amendment filed on 02/12/07 have been entered and made of record. Therefore, presently pending claims are 1-28.

Response to Arguments

Applicant's arguments filed 02/12/07 have been fully considered. There is new prior art cited. The newly cited prior art will overcome the shortcomings of Nikander.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-13, 17-23, and 27 are rejected under 35 U.S.C. 102(a) as being anticipated by the article by Montenegro et al ("Statistically Unique and Cryptographically Verifiable (SUCV) identifiers and addresses").

In reference to claim 1 Montenegro discloses a method of addressing the identifier ownership problem by using characteristics of Statistic Uniqueness and Cryptographic Verifiability wherein the SUCV addresses can solve the address ownership problem (Introduction). The system includes providing a private key and public key pair at a first node (Section 7 paragraph 1), Generating, by the first node, and address using the public key of the first node (Section 7 paragraph 4), and Providing said address to a second node, receiving an

address verification request from a second node at said first node, and said first node proving to said second node that the first node owns said address by providing an address verification answer generated using said private key corresponding to said public key (Section 6.2).

In reference to claims 17 and 27, the node including a providing unit configured to provide a private key and a public key pair (section 5.1),

an address generating unit configured to generate the address using the public key of the node (section 5.2 in combination with section 3),

an answer generating unit configured to prove ownership of the address by providing an address verification answer to at least one address verification request sent by a second node, the answer being generated using the private key corresponding to the public key (Section 6.2 paragraphs 4-6); wherein Montenegro teaches that the MN signs message with the private key of the private and public key pair that is used to produce the sucvHID (address generated using the public key).

In reference to claims 2 and 18, wherein the address generating unit comprises a computing unit configured to compute an address generation value using the public key, and a generating unit configured to generate an address, preferably a dynamic address, using said address generation value (section 5).

In reference to claims 4 and 19, the answer generating unit configured to generate the private and public key according to an identification protocol (section 5).

In reference to claims 5 and 20, wherein the identification protocol is a zero-knowledge identification protocol (section 6.1).

In reference to claims 3 and 21, wherein the address is an Ipv6 (IP version 6) address (Section 5.2).

In reference to claims 6 and 22 wherein the computing is further configured to compute, as the function using the public key, a hash of the public key (Section 7)

In reference to claims 7 and 23 wherein the address generating unit is further configured to use the computing result as the suffix of the address generated by the node (Section 5.2).

In reference to claim 8 wherein said address verification request sent by said second node includes a cookie and a challenge (section 6.2). Cookie is a text file, and Montenegro discloses sending the information in the message which is text and therefore in the cookie format.

In reference to claim 9 wherein said cookie is computed by said second node using a security algorithm and a security key of said second node (section 6.2)

In reference to claim 10 wherein said challenge is a random number (section 6.2).

In reference to claim 11 wherein said first node computes a response by applying said private key to said challenge (section 6.2).

In reference to claim 12 wherein said first node sends an address verification response including said cookie, said response and said public key (section 6.2).

In reference to claim 13 wherein said second node verifies that said first node owns said address by computing a hash of said public key and comparing the resulting value with said address generating value in a suffix of said dynamic address, and by applying said public key and comparing the result with a challenge (section 8.2.2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 14-15, 24-25, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montenegro in view of the article by Mortensen ("Password Protection Is This The Best We Can Do?").

In reference to claims 14, 24, and 28, Montenegro discloses a system to solve the address ownership problem (Introduction 1). The system generates the IP address based on a public key (section 8.2.1); receiving by another node the IP address thereby verifying that the node owns the IP address by checking the key (section 6.2).

Although Montenegro discloses the use of a key, Montenegro does not disclose the use of a passwords used only once.

Mortensen discloses the use of a password used only once (Section: One Time Password).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the one time password as in Mortensen in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because the combination of something you know and something you have provide a strong two factor authentication into computer systems (Mortensen: One Time Password) and therefore provide strong authentication of the owner of the address of Montenegro.

In reference to claims 15 and 25, wherein the node generates the IP address using an advertised network prefix and the key as the suffix Montenegro (Section 5.2).

Although Montenegro discloses the use of a key, Montenegro does not disclose the use of a passwords used only once.

Mortensen discloses the use of a password used only once (Section: One Time Password).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the one time password as in Mortensen in the system of Montenegro. One of ordinary skill in the art would have been motivated to do this because the combination of something you know and something you have provide a strong two factor authentication into computer systems (Mortensen: One Time Password) and therefore provide strong authentication of the owner of the address of Montenegro.

Claims 16 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Montenegro in view of the article by Mortensen as applied to claim 14 and further in view of Nikander (20020133607A1).

In reference to claims 16 and 26 Montenegro does not discloses a node that includes a number into the generated IP address, the number being incremented or decremented each time the IP address is transmitted to the another node, the another node additionally checking the number for verifying ownership of the IP address.

Nikander discloses "A method of claim 14 and 24, wherein the node includes a number into the generated IP address, the number being incremented or decremented each time the IP address is transmitted to the another node, the another node additionally checking the number for

verifying ownership of the IP address" in (Para 0104-0105) [TTLA is time to live value in RFC2373]

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify Mortensen's invention to incorporate Nikander's teaching of implementing a secure public key system to authenticate the IP address of a host. One of ordinary skill in the art would have been motivated to do this because it ensures a high fidelity of ownership of the IP address

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PWK
Monday, May 14, 2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100